Tk

UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/042,019	01/08/2002	Zheng Qi	2875.0680001	4910

26111 7590 12/22/2006
STERNE, KESSLER, GOLDSTEIN & FOX PLLC
1100 NEW YORK AVENUE, N.W.
WASHINGTON, DC 20005

EXAMINER	
COLIN, CARL G	
ART UNIT	**PAPER NUMBER**
2136	

SHORTENED STATUTORY PERIOD OF RESPONSE	MAIL DATE	DELIVERY MODE
3 MONTHS	12/22/2006	PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

If NO period for reply is specified above, the maximum statutory period will apply and will expire 6 MONTHS from the mailing date of this communication.

Office Action Summary	**Application No.** 10/042,019	**Applicant(s)** QI, ZHENG	
	Examiner Carl Colin	**Art Unit** 2136	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *10 October 2006*.

2a)☒ This action is **FINAL**. 2b)□ This action is non-final.

3)□ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-24* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)□ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-24* is/are rejected.

7)□ Claim(s) _____ is/are objected to.

8)□ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)□ The specification is objected to by the Examiner.

10)□ The drawing(s) filed on _____ is/are: a)□ accepted or b)□ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)□ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)□ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)□ All b)□ Some * c)□ None of:

1.□ Certified copies of the priority documents have been received.

2.□ Certified copies of the priority documents have been received in Application No. _____.

3.□ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) □ Notice of References Cited (PTO-892)

2) □ Notice of Draftsperson's Patent Drawing Review (PTO-948)

3) □ Information Disclosure Statement(s) (PTO/SB/08)
Paper No(s)/Mail Date _____.

4) □ Interview Summary (PTO-413)
Paper No(s)/Mail Date. _____ .

5) □ Notice of Informal Patent Application

6) □ Other: _____.

DETAILED ACTION

Response to Arguments

1. In response to communications filed on 10/10/2006, applicant amends claims 1, 2, 7-10, 13-15, 18, and 22. The following claims 1-24 are presented for examination.

2. In response to communications filed on 10/10/2006, the 112th rejection first paragraph of claims 23-24 have been withdrawn. Upon further consideration, the double patenting rejection has been withdrawn.

2.1 Applicant's remarks, pages 8-12, filed on 10/10/2006, with respect to the 102 and 103 rejection of claims 1-24 have been fully considered but they are not persuasive. Applicant mentions on page 10 of the remarks that the claims have been amended to recite a combined adder tree that has two parallel outputs, and Kang fails to teach a combined adder tree having two parallel outputs. Examiner respectfully disagrees. The 512-bit registers of figure 2 show two multiplexers (Mux-3 and Mux-Wt) providing two outputs in parallel, which meet the claimed limitation as amended. Also, it is reasonable to say that the combined adder tree of figure 2 has two parallel output multiplexers one from each buffer: Mux-1 from the 160-input buffer and Mux-3 from the 512-input buffer, which are added to the 32x5 adder. Therefore, applicant has not overcome the rejection of independent claims 1 and 10 in view of Kang. Applicant adds that the other claims because of their dependency to claims 1 and 10 are patentable over Kang for the same reason discussed above. Claims 1-24 are still rejected in view of the prior art. Upon further consideration, the claims are rejected as set forth below.

Claim Rejections - 35 USC § 103

3. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

(a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

Claims 1-7, 10-12, 16, and 23-24 are rejected under 35 U.S.C. 103(a) as being unpatentable over non-Patent Literature "An Efficient Implementation of Hash Function Processor for IPSEC" to Kang et al, pp. 1-4.

As per claim 1: Kang et al discloses an authentication engine architecture for a SHA-1 multi-round authentication algorithm, comprising: a hash engine configured to implement hash round logic for an SHA1 authentication algorithm, the hash round logic implementation including, a combined adder tree (see for instance, figure 2). As interpreted by the Examiner Kang et al suggests using a high speed adder with 8-bit CLA to minimize delay the path taken with the high speed adder meets the recitation of a timing critical path having a single 32-bit carry look-ahead adder (CLA) (see page 2, paragraph above fig. 3), wherein said combined adder tree has two parallel outputs; the 512-bit registers of figure 2 shows two multiplexers (Mux-3 and Mux-Wt) providing two outputs in parallel, (see complete pages 1-2, sections 2-3 for details). Also, it is reasonable to say that the combined adder tree of figure 2 has two parallel output multiplexers one from each buffer: Mux-1 from the 160-input buffer and Mux-3 from the 512-input buffer, which are added to the 32x5 adder. Although Kang et al discloses a 8-bit CLA instead of a 32-bit CLA, it is apparent to one of ordinary skill in the art that the number of bits may be chosen as a matter of design choice because it only requires routine skill in the art to modify the architecture to use different numbers of bit inputs in the adder to meet the design choice.

As per claim 2: Kang et al discloses in (section 3.1 column 2), to minimize the adder delay we implemented high speed adder using CLA, CSA, and carry select adder (multiplexer operation) that meets the recitation of a timing critical path equivalent to one of: 5-bit addition, one 32-bit CSA, a multiplexer operation, and one-32 bit CLA and three 32-bit CSAs, a multiplexer operation, and one-32 bit CLA (see sections 3.1-3.3 and figs. 2-3 and 5). It is apparent to one of ordinary skill in the art that the number of registers or bits may be chosen as a matter of design choice because it only requires routine skill in the art to modify the architecture to use different numbers of bit inputs in the adder, or multiplexers to meet the design choice.

As per claim 3: Kang et al discloses the limitation of wherein the additions performed by the combined adder tree are preceded by a 5-bit circular shifter (see fig. 2).

As per claim 4: Kang et al discloses the claimed apparatus of claim 3, and further discloses the combined adder tree includes add5to1 (see for instance 32x5 adder of figure 2) and add4to1 adders (see for instance 32x4 adder of figure 5). It is apparent to one of ordinary skill in the art that the number of registers or bits may be chosen as a matter of design choice because it only requires routine skill in the art to modify the architecture to use different numbers of adder bits to meet the design choice.

As per claim 5: Kang et al discloses the limitation of wherein the combined adder tree is configured such that addition computations are conducted in parallel with round operations (section 3.1).

As per claim 6: Kang et al discloses the authentication engine architecture of claim 1, wherein the architecture is implemented as an authentication engine architecture for a multi-loop, SHA-1 authentication algorithm comprising: Kang et al discloses in figures 2 and 5-7 two loops of operation (left side and right side of each figure) that meets the recitation of *a first instantiation of a SHA-1 authentication algorithm hash round logic in an inner hash and a second instantiation of an SHA-1 authentication algorithm hash round logic in an outer hash engine* (see sections 3.1-3.3 and figs. 2-5); and further discloses two input buffers (see figure 2) that meets the recitation of *a dual-frame payload data input buffer configured for loading one new* *data block while another data block one is being processed in the inner hash engine* (see section 3.1); also discloses loading hash states in the 512-bit and 160-bit modules (see section 3.1 and figure 2) that meets the recitation of *an initial hash state input buffer configuration for loading initial hash states to the inner and outer hash engines for concurrent inner hash and outer hash operations*; Kang et al discloses a Rom for storing constant in figure 2 that meets the recitation of *a dual-ported ROM configured for concurrent constant lookups for both inner and outer hash engines* (see section 3.1). Although not shown in the figures or explicitly cited a dual-port memory for both modules, it would have been obvious to one of ordinary skill in the art at the time the invention was made to use a shared memory for implementing parallel operation as suggested in section 3.1. Kang et al discloses an architecture configured for parallel processing and two separate input buffers (see section 3.1). Although not explicitly stated loading one new data block while another data block one is being processed in the inner hash engine, as the term parallel processing is well known in the art, it is apparent to one of ordinary skill in the art that Kang et al's architecture is configured to perform parallel processing such as loading one new data block while another data block one is being processed. Therefore, it would have been obvious to one of ordinary skill in the art to load one new data block while another data block one is being processed to save in processing time by performing parallel processing as suggested by Kang et al.

As per claim 7: Kang et al discloses the authentication engine architecture of claim 6, wherein the multi-loop, multi-round authentication algorithm is HMAC-SHA1 (see section 1).

As per claim 10: Claim 10 is similar to claim 1 except for implementing the claimed apparatus into a method. Kang et al discloses receiving a data packet stream, splitting the packet data stream into fixed-size data blocks (see section 2.3); and processing the fixed-size data blocks using a SHA-1 multi-round authentication engine architecture, said architecture implementing hash round logic for a SHA1 authentication algorithm including a combined adder tree (see for instance, figure 2) with a timing critical path having a single 32-bit carry look-ahead adder (CLA) (see page 2, paragraph above fig. 3), wherein said combined adder tree has two parallel outputs; the 512-bit registers of figure 2 shows two multiplexers (Mux-3 and Mux-Wt) providing two outputs in parallel, (see section 2.1-3.2 for complete details).

As per claim 11: Kang et al discloses the claimed method of claim 10. Claim 11 recites the same limitations as claim 2 and is rejected on the same rationale as the rejection of claim 2.

As per claim 12: Kang et al discloses the limitation of wherein the additions performed by the combined adder tree are preceded by a 5-bit circular shifter (see fig. 2).

As per claim 16: Kang et al discloses the limitation of wherein the combined adder tree is configured such that addition computations are conducted in parallel with round operations (section 3.1).

As per claim 23: Kang et al discloses a multiplexer and select signal to the multiplexer for selecting output of combined adder tree that meets the recitation of comprising a multiplexer to select an output of the combined adder tree (see for example, figures 1 and 6).

As per claim 24: Kang et al discloses a multiplexer operation to provide an output of the combined adder tree (see for example, output from the Mux in figures 1 and 6).

4. **Claims 8-9, 13-15, 17-22** are rejected under 35 U.S.C. 103(a) as being unpatentable over non-Patent Literature "An Efficient Implementation of Hash Function Processor for IPSEC" to Kang et al, pp. 1-4 as applied to claim 1 above, in view of Schneier "Applied Cryptography, Second Edition", John Wiley & Sons, New York, 1996, Pages 436-445.

As per claims 8-9, & 15: Kang et al discloses five hash state registers; and discloses implementing parallel processing (figure 2 and section 3.1) and using one path that is not a critical path as illustrated in figs. 2-4, thereby collapse the number of rounds that meets the recitation of wherein eighty rounds of an SHA1 loop are collapsed into forty rounds (see sections 2.1-3.2 and figs. 2-4). Kang et al does not explicitly state one critical and four non-critical data paths associated with the five registers, such that in successive SHA1 rounds, registers having the critical path are alternative because in Kang et al they are well known or inherent features of the architecture disclosed. Schneier in an analogous art teaches the basic concept of SHA that providing more detailed explanation and discloses one critical and four non-critical data paths associated with the five registers, such that in successive SHA1 rounds, registers having the critical path are alternative. Figure 18.7 for instance, shows only one SHA operation for illustration purpose, the architecture comprises one timing critical path (ei-1 to ai) out of the five data paths, but as (i) changes, on each operation only one register receives the critical path making the critical path alternative. (See Pages 442-445). Therefore it would have been obvious to one ordinary skilled in the art at the time the invention was made to apply Schneier concept of secure hash algorithm description that is well known in the art in the system of Kang et al. One of ordinary skill in the art would have been motivated to do so in order to ensure of the security of the messages being sent and exchanged in the system and to save in processing time (Page 442).

As per claims 13-14: Kang et al discloses five hash state registers; and discloses implementing parallel processing (figure 2 and section 3.1) and using one path that is not a critical path as illustrated in figs. 2-4, thereby collapse the number of rounds that meets the recitation of wherein eighty rounds of an SHA1 loop are collapsed into forty rounds (see sections 2.1-3.2 and figs. 2-4). Kang et al does not explicitly state one critical and four non-critical data paths associated with the five registers, such that in successive SHA1 rounds, registers having the critical path are alternative because in Kang et al they are well known or inherent features of the architecture disclosed. Schneier in an analogous art teaches the basic concept of SHA that providing more detailed explanation and discloses one critical and four non-critical data paths associated with the five registers, such that in successive SHA1 rounds, registers having the critical path are alternative. Figure 18.7 for instance, shows only one SHA operation for illustration purpose, the architecture comprises one timing critical path (ei-1 to ai) out of the five data paths, but as (i) changes, on each operation only one register receives the critical path making the critical path alternative. (See Pages 442-445). Therefore it would have been obvious to one ordinary skilled in the art at the time the invention was made to apply Schneier concept of secure hash algorithm description that is well known in the art in the system of Kang et al. One of ordinary skill in the art would have been motivated to do so in order to ensure of the security of the messages being sent and exchanged in the system and to save in processing time (Page 442).

As per claim 17: Kang et al discloses the claimed method of claim 10 and further discloses wherein said authentication engine architecture is a multi-loop multi-round authentication engine architecture having a hash engine core comprising *an inner hash engine and an outer hash engine* Kang et al discloses in figures 2 and 5-7 two loops of operation (left side and right side of each figure) that meets the recitation of *a first instantiation of a SHA-1 authentication algorithm hash round logic in an inner hash and a second instantiation of an SHA-1 authentication algorithm hash round logic in an outer hash engine* (see sections 3.1-3.3 and figs. 2-5); *configured to implement multi-round logic such that addition computations are conducted with round operations* (section 3.1). and configured to *pipeline hash operations of said inner and outer hash engines* (see for instance fig. 6 and 7), and discloses implementing parallel processing (figure 2 and section 3.1) and using one path that is not a critical path as illustrated in figs. 2-4, thereby collapse the number of rounds that meets the recitation of *collapse and rearrange multi-round logic to reduce rounds of hash operations* (see sections 2.1-3.2 and figs. 2-4). Schneier in an analogous art teaches the basic concept of SHA that providing more detailed explanation and discloses one critical and four non-critical data paths associated with the five registers, such that in successive SHA1 rounds, registers having the critical path are alternative. Figure 18.7 for instance, shows only one SHA operation for illustration purpose, the architecture comprises one timing critical path (ei-1 to ai) out of the five data paths, but as (i) changes, on each operation only one register receives the critical path making the critical path alternative. (See Pages 442-445). Therefore it would have been obvious to one ordinary skilled in the art at the time the invention was made to apply Schneier concept of secure hash algorithm description that is well known in the art in the system of Kang et al. One of ordinary skill in the art would have been motivated to do so in order to ensure of the security of the messages being sent and exchanged in the system and to save in processing time (Page 442).

As per claim 18: The references as combined above disclose the claimed method of claim 17. Kang et al discloses wherein the multi-loop, multi-round authentication algorithm is HMAC-SHA1 (see section 1).

As per claim 19: The references as combined above disclose the claimed method of claim 18. Kang et al discloses implementing parallel processing (figure 2 and section 3.1) (see also figures 5 and 6 where data input for each hash engine is performed in parallel.

As per claims 20-22: claims 20-22 recite similar limitation as interpreted by the Examiner as found in claim 6. Therefore, these claims are rejected on the same rationale as the rejection of claim 6. Claim 19 recites similar limitation as found in claims 6, 9, and 13 as per pipelining or parallel processing of operations with inner and outer hash engine.

Conclusion

5. Any inquiry concerning this communication or earlier communications from the examiner should be directed to Carl Colin whose telephone number is 571-272-3862. The examiner can normally be reached on Monday through Thursday, 8:00-6:30 PM.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Nasser G. Moazzami can be reached on 571-272-4195. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

Carl Colin
Patent Examiner
December 19, 2006

NASSER MOAZZAMI
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100

12/19/06